REMARKS

In a Final Office Action mailed 30 November 2005, the Examiner rejected claims 16 and 17 under 35 USC §102(b) as being anticipated by Chang et al. (US Patent No. 5,724,425). The Examiner also rejected claims 1 – 5, 10 – 14, 16, and 17 under 35 USC §103(a) as being unpatentable over Chang et al. (US Patent No. 5,724,425), and further in view of Ho et al. (US Patent Application Publication No. 2002/0073325), and claims 6 – 9, 15, and 18 under 35 USC §103(a) as being unpatentable over Chang et al. (US Patent No. 5,724,425), and Ho et al. (US Patent Application Publication No. 2002/0073325), as applied to claim 1 above, and further in view of Horstmann (US Patent No. 6,044,469).

Anticipation Rejection of Claims 16, 17

The Examiner rejected claims 16 and 17 under 35 U.S.C. §102(b) as being anticipated by Chang et al. (US Patent No. 5,724,425) noting with respect thereto:

> Regarding claims 16 and 17: Hashing a file to produce a hash value (Col 7 lines 1-20) a message digest is used to describe the process of hashing the file. Chang et al. states that any known message digest algorithm such as MD2, MD4, or MD5 may be used in the creation of the digest. These algorithms hash the file in this same manner as described by the applicant thus providing for a hash value as the resultant. Encrypting the hash value with a key to generate a signature (Col 7 lines 1-5). Comparing the generated signature with the original (Fig 6(a, b), Col 9 lines 37-47) Chang et al states that the file is hashed (i.e. message digest generated) and the signature is decrypted to provide the original hash value. In this manner Chang et al provides for that which is claimed since these are to same thing by way of a logical transitive relationship. Encrypting the newly generated hash value and comparing that to the provided signature is logically the same as decrypting the original signature and comparing that to the produced hash value.

Applicants have carefully reviewed the Examiner's rejections and the cited Chang reference. Applicants have canceled claims 16 and 17.

Obviousness Rejection of Claims 1 – 15 and 18

The Examiner rejected claims 1 – 5, 10 – 14, 16, and 17 under 35 U.S.C. §103(a) as being anticipated by Chang et al. (US Patent No. 5,724,425) and further in view of Ho et al (US Patent Publication No. 2002/0073325), and claims 6 – 9, 15, and 18 under 35 USC §103(a) as being unpatentable over Chang et al. (US Patent No. 5,724,425), and Ho et al. (US Patent Application

Publication No. 2002/0073325), as applied to claim 1 above, and further in view of Horstmann (US Patent No. 6,044,469). The Examiner noted with respect thereto:

> Chang et al ("Chang") has taught the method of authentication as in the claimed invention, but fails to teach the implementation of an owner key that is unique to the given computer system.
>
> Ho et al ("Ho"), however teaches the use of a key specific to the individual computer system for the purposes of license integrity.
>
> It is desirable to maintain the authenticity of a software program from malicious attack by worms, viruses and other programs or individuals that have the common intent of harming a host system. Such programs are known to often compromise critical information of such a system and cause additional damage. As taught by Chang et al such attacks are avoidable by the implementation of a signature system that is composed of a message digest to confirm the integrity of the software. Ho teaches that a greater level of security may be obtained by the implementation of a unique key signature of a system so as to prevent that particular license from being compromised (Ho paragraphs 4-12, Chang Col. 1 line 50-Col 3 line 13).

Applicants have carefully reviewed the Examiner's rejections and the cited Chang reference. Applicants have amended the independent claims to distinguish Applicants' invention from the teachings of the cited references and provide the following remarks in support of patentability of the claimed invention.

Applicants' secure data authentication apparatus provides a method for authenticating the source of a software file as well as the owner of the software file and the telephony switching system on which the software file is being installed. The software file is hashed using a selected hash algorithm. The hash value is then encrypted with the unique owner key to calculate a source signature. The benefit of creating a unique owner signature to append to the installation software is to prevent unauthorized individuals that obtain the software file in an unscrambled form from using the software file without authorization. Once calculated, the source signature and/or unique owner signature are appended to the software file. A secure microprocessor is located within the telephony switching equipment and includes an encryption algorithm, a security routine, a source key, and the unique owner key that are used by the secure microprocessor to calculate a source signature and a unique owner signature for each software file or downloaded image. The secure microprocessor compares the calculated source and owner signatures to the source and owner signatures appended to the end of the software file or images. If the signatures match, installation and use is authorized. If the signatures do not match, the software file cannot be installed and the telephony switching system may be disabled.

The use of an owner's key that is unique to each telephony switching system, which unique owner's key is used to encrypt the hash value at the source and also at the secure processor at the telephony switching system, is neither shown or suggested by the cited references. This limitation is now clearly recited in the independent claims, claim 1 of which is an example:

> 1. A secure data authentication apparatus to authenticate a software file, the software file having a first signature appended to the software file, for use on a computer system, wherein said computer system is assigned an owner key that is unique to said computer system, said first signature comprising a source hash value that is computed by processing at least some of said software file using a selected hash function, which source hash value is encrypted using said owner key to produce said first signature, the apparatus comprising:
>
> a secure processing device within the computer system to receive the software file and hash the software file using said selected hash function to produce a first hash value; and
>
> a first key located within the secure processing device, which first key comprises said owner key wherein the secure processing device encrypts the first hash value with the first key to generate a second signature and compares the first signature with the second signature, and if the first signature matches the second signature, the computer system accepts the software file as being authenticated.

The cited Chang patent teaches that, to protect a source code file, a software application writer's private key, along with an application writer's license, is provided to a first computer. The application writer's license includes identifying information, such as the application writer's name, as well as the application writer's public key. A compiler program executed by the first computer compiles the source code into binary code and computes a message digest for the binary code. The first computer then encrypts the message digest using the application writer's private key, such that the encrypted message digest is defined as a digital "signature" of the application writer. A software passport is then generated which includes the application writer's digital signature, the application writer's license, and the binary code. A user, upon receipt of the software passport, loads the passport into a computer, and the user's computer computes a second message digest for the software passport and compares it to the first message digest, such that if the first and second message digests are not equal, the software passport is also rejected by the user's computer and the code is not executed. However, as noted by the Examiner, "Chang ... fails to teach the implementation of an owner key that is unique to the given computer system," which structure is affirmatively recited in Applicants' independent claims.

The Examiner relies on the cited Ho patent that teaches:

> A method and an apparatus for using an encrypted unique digital signature ("engraved signature") as a uniquely definable signature to control the use or execution of software in a computer system. The computer system has a Network Interface Card ("NIC") with a Media Access Control ("MAC") address. On start up, the engraved signature is retrieved from the persistent storage medium of the computer system and the MAC address is retrieved from the NIC. A computed encrypted signature is generated using the MAC address. Where the computed encrypted signature does not match the engraved signature, the execution of the software is halted. (Abstract)

However, the Ho patent is limited to a self-contained storage medium and a network interface card, as noted in paragraphs [0008] – [0010]:

> [0008] The problem of software piracy is acute with a particular class of computer systems: Internet Appliances. An Internet Appliance is generally a computer system that performs some predetermined functions while connected to the Internet. The Internet Appliances typically consist of computer hardware with embedded software. The hardware includes a storage medium and a network interface card.
>
> [0009] Software embedded in an Internet Appliance tends to be compact. It is not uncommon to store the entire system software in a storage medium that has only a few megabytes of capacity. This type of storage medium is usually small and very portable (such as CompactFlash and SIM cards). Because of wide adaptation and portability of such media, digital content inside such mediums can be illegally duplicated very easily.
>
> [0010] It is therefore an aspect of an object of the present invention to provide a method and an apparatus for protecting the embedded software in computer systems, such as Internet Appliances, against unauthorized use, while being relatively cost-effective to deploy.

The Ho patent further notes that it is impractical to execute a unique compilation of the software for each computer:

> [0005] Restricted entitlement means that the software contains some means to limit itself to run only on the computer system for which it is authorized. A common restriction method is to encode hardware specific information in the computer system so that the software can verify the information at system startup. Another method is to make the software unique for every computer system. This entails unique compilation of the software for each distribution, which is a very costly operation.

Therefore, the Ho patent specifically rejects the combination noted by the Examiner, since the use of a computer-specific encoding is impractical. Instead, the Ho patent relies on the

fact that the target type of software is Internet Appliance where "The Internet Appliances typically consist of computer hardware with embedded software. The hardware includes a storage medium and a network interface card." Thus, the Ho patent relies on the software to be distributed as part of the hardware of the Internet Appliance and does not envision transmission of programs over a network to the end user computer.

In contrast, Applicants' secure data authentication apparatus makes use of a file transmission protocol where "the software file having a first signature appended to the software file", and the user's "computer system is assigned an owner key that is unique to said computer system." The hash value is computed "by processing at least some of said software file using a selected hash function, which source hash value is encrypted using said owner key to produce said first signature." Thus, when the user's computer receives the software file and the associated digital signature, it can recompute the digital signature and compare it to the received digital signature. Thus, Applicants' independent claim 1 recites structure that is not shown or suggested by the cited references, since the Ho patent specifically teaches away from the combination suggested by the Examiner. As required for a valid obviousness rejection, the MPEP and courts have stated that the Examiner must show the following:

> 1.) A motivation or suggestion to combine references, 2.) A reasonable expectation of success from combining the references, and 3.) The combined references teach all of the limitations of the claimed invention. MPEP §706.02(j); see also *In re Vaeck*, 20 USPQ2d 1438 (Fed. Cir. 1991).

In order to meet the first of the above-noted three requirements by the MPEP for prima facie obviousness, the following must be shown: 1.) one or more references, 2.) the references were available to the inventor at the time of the claimed invention, 3.) each of the references teaches an element of the claimed invention, 4.) the prior art contains a suggestion or a motivation to combine the references, 5.) the combination of the references would have made the invention obvious. See *In re Rinehart*, 189 USPQ 143, 147 (C. C. P. A. 1976); *In re Fine*, 5 USPQ2d 1596, 1598 (Fed. Cir 1988); *In re Fitch*, 23 USPQ2d 1780, 1783 (Fed. Cir. 1992).

Since the cited references fail element 4. noted above, Applicants therefore believe that claims 1 – 15 and 18 are allowable under 35 USC §103(a) over the cited references for the reasons noted above.

In view of the above amendments and remarks, Applicants believe the pending application is in condition for allowance. Applicants believe no fee is due with this response. However, if a fee is due, please charge our Deposit Account No. 50-1848, under Order No. 013217.0177PTUS from which the undersigned is authorized to draw.

Respectfully submitted,
PATTON BOGGS LLP

Dated: 06- February - 2006

By: _____
James M. Graziano
Registration No.: 28,300
(303) 830-1776
(303) 894-9239 (Fax)
Attorney for Applicants

Customer No. 24283